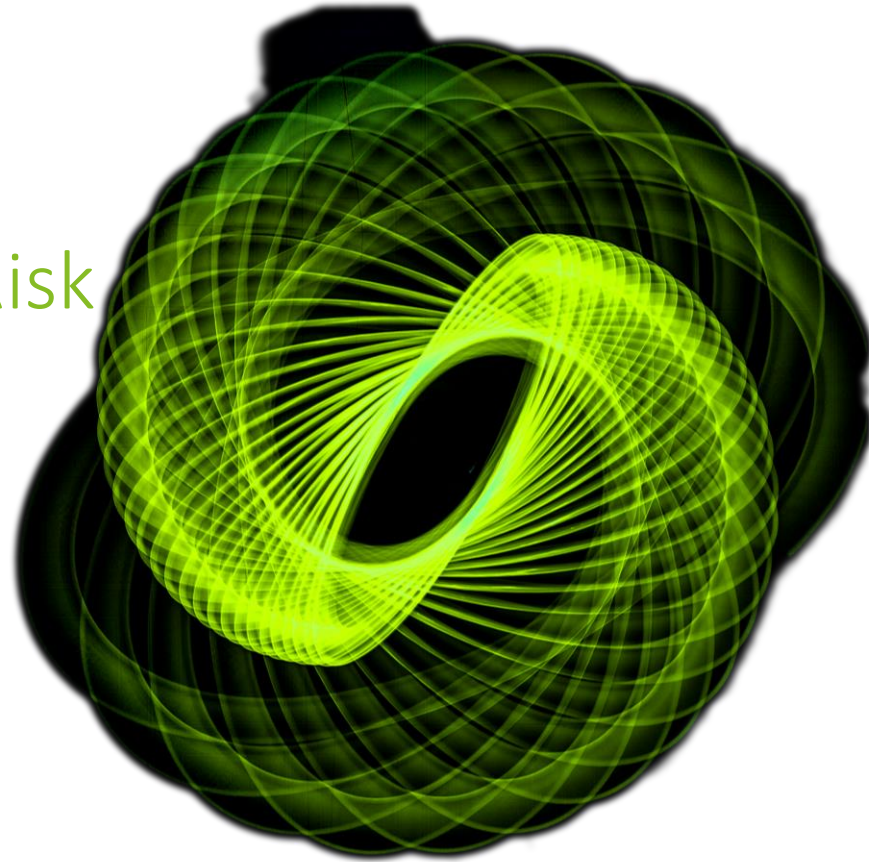



## clQ – Next Generation Cyber Risk Management



The background of the slide is a complex geometric pattern. It features a network of light blue lines connecting various points, forming a series of triangles and hexagons. Scattered throughout this network are several solid-colored hexagons in shades of green, blue, and grey. Some of these hexagons are larger and more prominent, while others are smaller and serve as nodes in the network. The overall effect is a modern, tech-oriented aesthetic.

Executives are now demanding those in  
charge of cyber security to financially  
quantify cyber risks facing their  
organizations

# Cyber risk quantification with cIQ

With rising cyber threats and a lack of methods to quantify the herewith related cyber risks, cIQ provides a validated and data-based approach to support companies in managing their cyber risks



## Cyber threats are on the rise...

15%

expected increase in economic impact of cyber-crimes per year over the next five years

€9T

estimated damage by cyber threats by 2025.



## ...yet cyber risk is not managed sufficiently...

81%

of board members believe their organization lacks sufficient protection



## ... and it cannot be quantified.

98%

of C-level managers cannot quantify cyber risks sufficiently

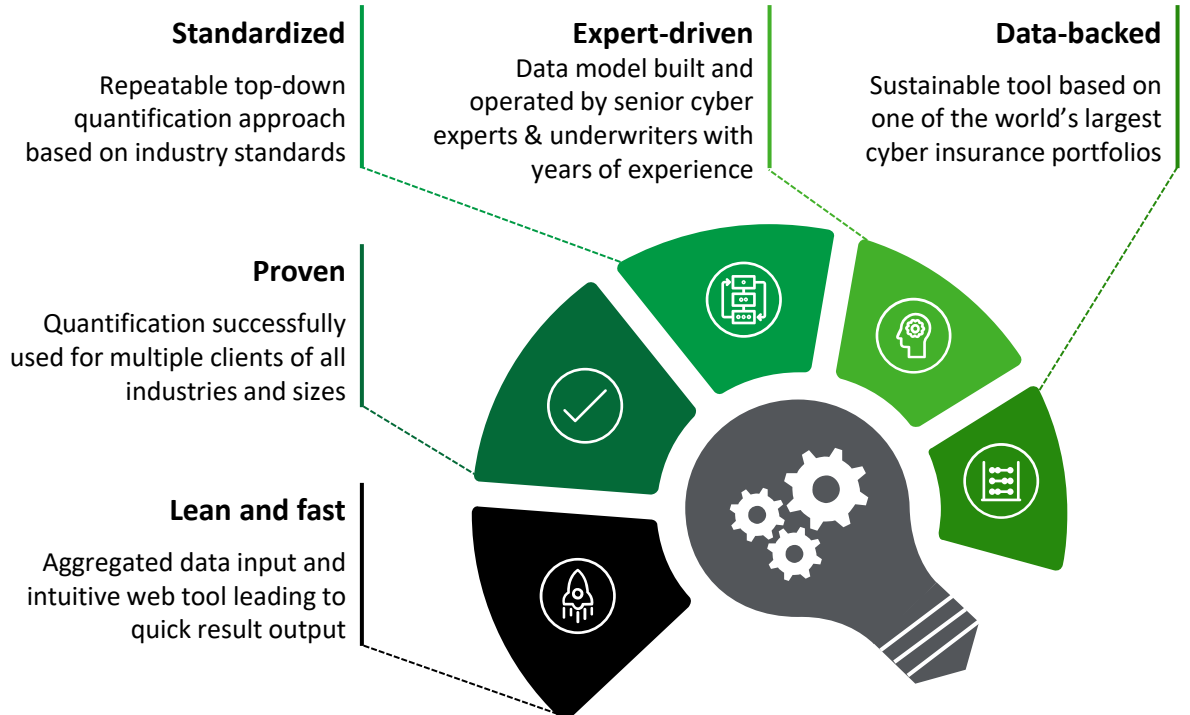
## Cyber Inspection & Quantification (cIQ) tool



cIQ enables leaders of complex companies to **efficiently manage their cyber risks** with quantified financial metrics

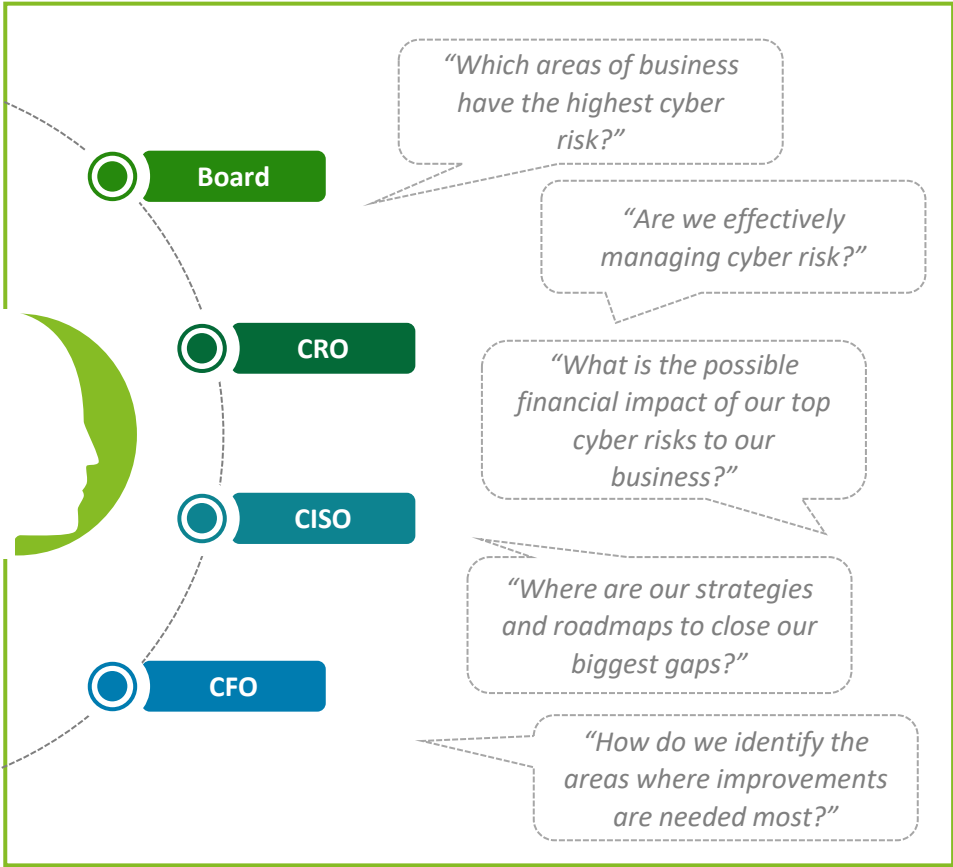


The **top-down approach** supports **strategic decision-making** and can complement existing bottom-up risk assessment



# clQ value proposition | Addressees and offerings

clQ offering supports in answering pressing questions by the board of management



## Cost Transparency

clQ provides an overview of the organization's exposure to cyber risks, a detailed analysis of their information security and risk metrics for their top risks

## Defense optimization

clQ enables detailed recommendations to improve the security posture by simulating the effects of possible security changes

## Risk monitoring

clQ is a standardized and repeatable approach that allows recurring assessments in order to monitor risks and track security improvements

## Scenario planning

clQ supports the organization in strategic decision-making by analyzing the defense capabilities and identifying top risk scenarios

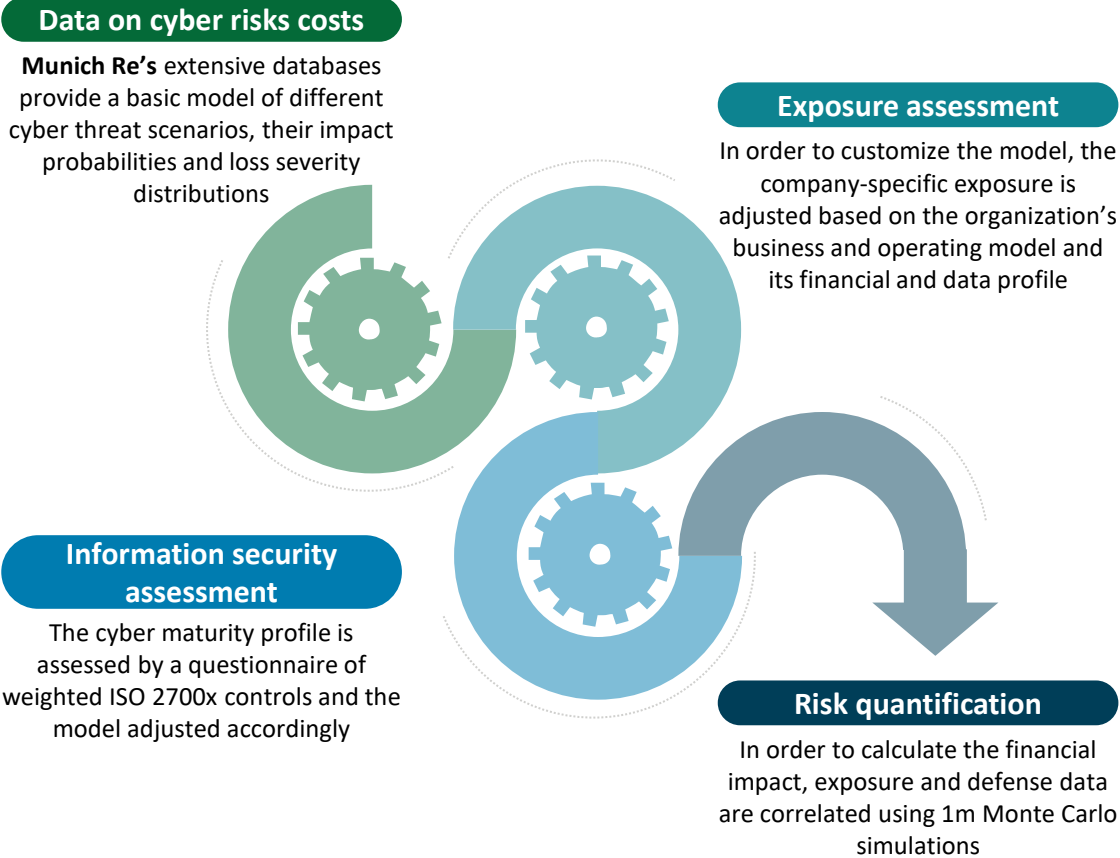


clQ leverages cyber risk quantification for strategic decision-making in cyber risk management

# clQ methodology and results

Leveraging an extensive database and years of cyber insurance experience, drivers and cost components of large cyber losses are identified and calibrated with company-specific assessments to provide valuable insights

## Methodology



## Results



**Cyber risk report**

- The final report provides valuable insights into the company profile, the exposure and maturity scores
- Summarizing the results of the quantification, simulated cyber events are detailed in the report with the respective impact and probabilities



**Quantified top cyber risks**

- A high-level overview of the top cyber risks is given, including an overall cyber score and risk metrics for business interruption, data breach, ransomware and financial theft & fraud scenarios



**Insights in Infosec posture and simulation results**

- Based on the company-specific information security posture, detailed recommendations for improvement are derived
- Simulation shows how cyber risk scores and metrics would change based on these recommendations

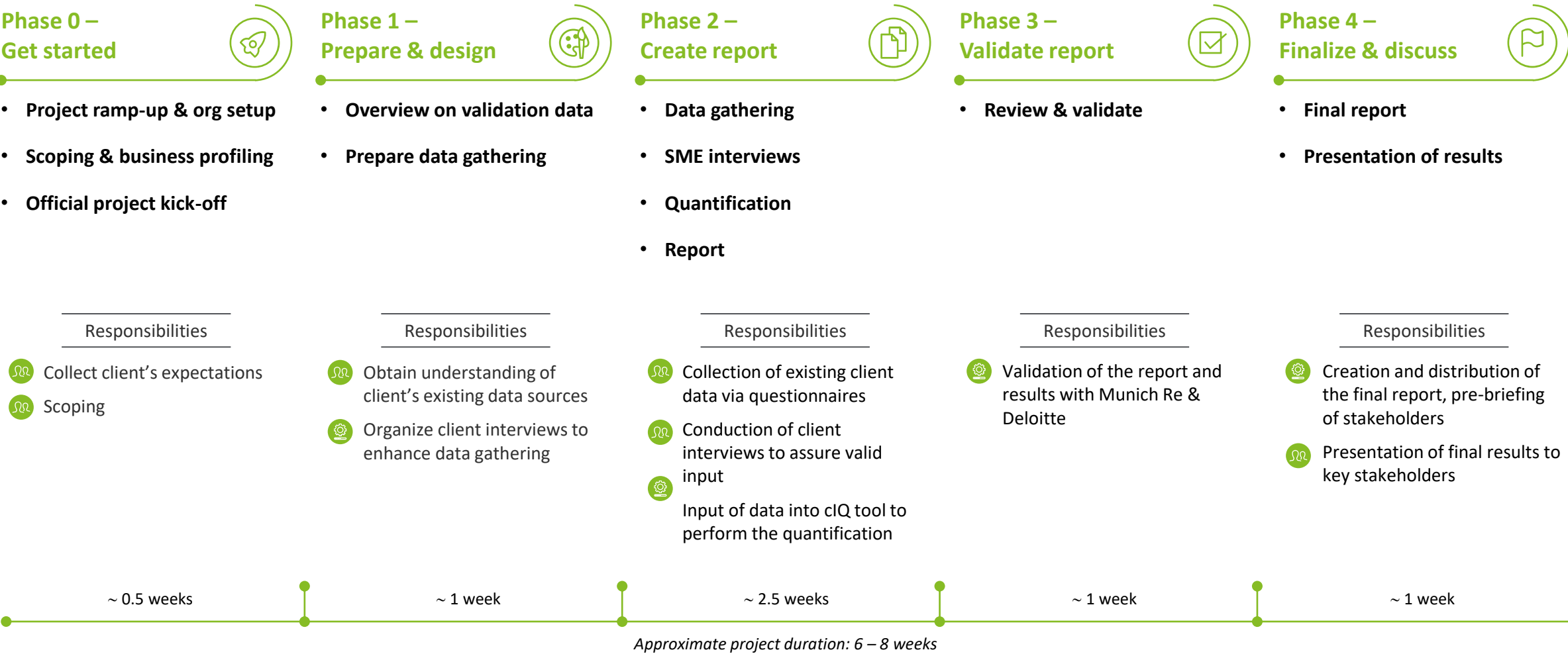


**Yearly assessments for measuring progress**

- Leveraging the repeatable and standardized process, yearly assessments can be executed to track progress
- With a steadily growing database, model accuracy is being improved continuously

# Approximate project timeline

A cIQ quantification project typically takes 6 – 8 weeks, depending on availability of company data as well as subject matter experts to provide the basis for the calculation



# Exemplary Outcomes

# Your Cyber Risk | Exemplary Worst Case Loss

As one of our financial loss metrics, the Worst Case Loss is the combination of extreme loss scenarios, in which almost all security measures fail

We model different types of risk. The Worst Case Loss is a scenario where we assume that almost all security measures would fail.


Therefore, these risk metrics are mainly calculated on the basis of exposure criteria.

If you decide to conduct a business impact analysis with us, the main risk drivers for such extreme financial losses can be identified.


Of course, this is a highly unlikely event. Still, being aware of the potential havoc such an incidence might create is a matter of responsibility. And looking at recent events, preparing for such an incident is of ever-growing importance.

For the calculation of the overall Worst Case Loss, the respective worst case losses of the three consequence scenarios are cumulated.


## Consequence Scenario<sup>1</sup>



As a result of stolen PCI/PHI data from the main customer database of US servers, confidential customer data and data on cost-intensive developments were published. Cost-intensive consequences arise, and costs spent on developing a new product line become obsolete



Due to stolen data, and hackers invading the system, the biggest manufacturing site in China cannot resume business as usual. Production stops for 6 months, non-compliance with contracts and costs to recover production are the consequences



Because of a vulnerability, unnoticed transfers could be carried out to fake suppliers over a period of three years. The transferred money can no longer be reclaimed



Data Breach



Business Interruption



Financial Theft

1 800M €

1 500M 2 100M

Worst Case Loss

Incident that would result in a maximal foreseeable loss



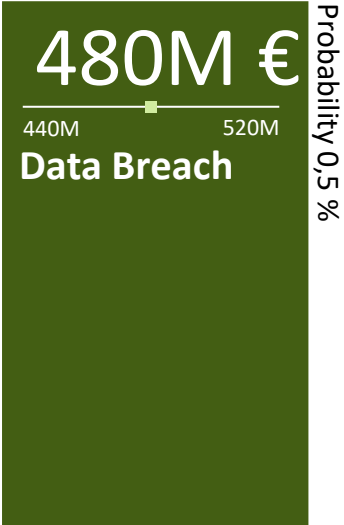
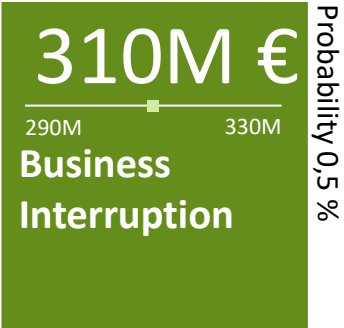
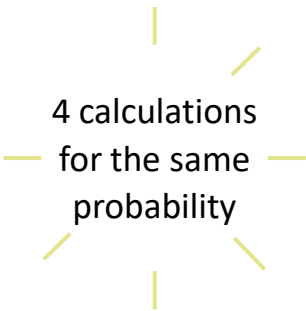
# Your Cyber Risk | Modelled Large Loss

As one of our financial loss metrics the Modelled Large Loss provides expected loss in relation to any specific probability, simulated over 1 000 000 years

In this example, taking into account similar industries and cyber incidents that we have observed and analyzed, we model the 1 in 200 years loss scenario\*.

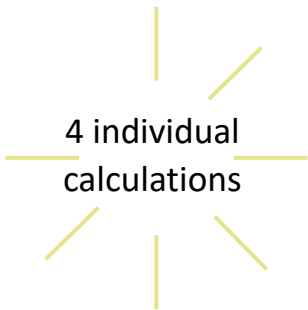
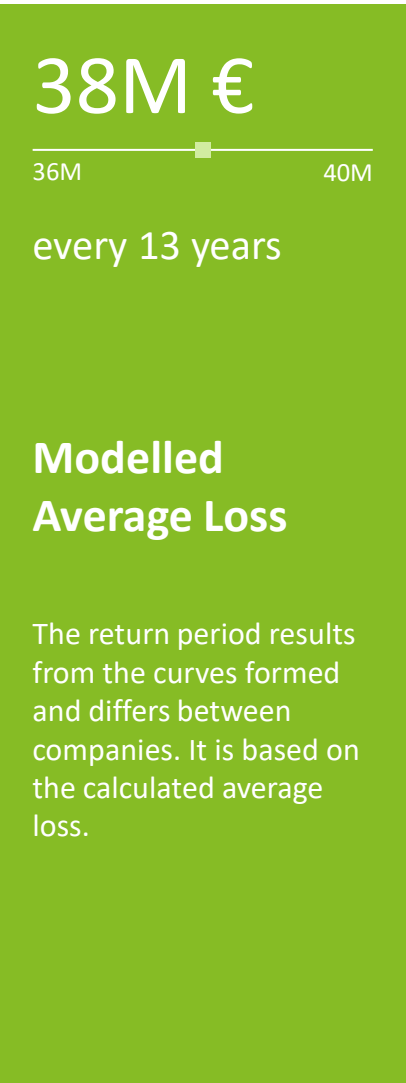
The expected value for all types of scenarios is calibrated to industry type and size, considering the loss and cost patterns of the industry classes.

The three most important consequence scenarios, Business Interruption, Data Breach, and Financial Theft are modelled individually and differently because frequency and severity of the three follow different patterns.



# Your Cyber Risk | Modelled Average Loss

Whereas the Modelled Large Loss includes all years of the Monte Carlo simulation, the Modelled Average Loss excludes years with significant losses



In order to ensure multiple meaningful measures of financial loss, we use the Modelled Average Loss in addition to the Modelled Large Loss.

In most companies' significant cyber losses do not occur every year. From the 1 million Monte Carlo simulations the Modelled Large Loss considers also simulations of years in which no or no significant loss is calculated. Also, for the calculation of the Average Loss all simulation years with highly significant losses are excluded.

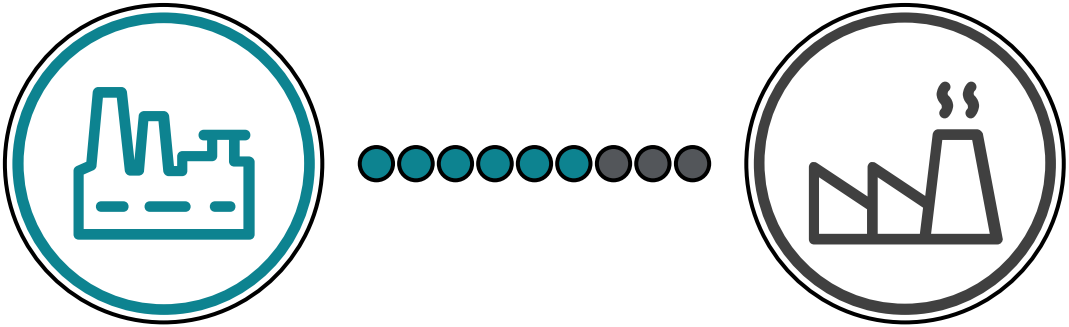
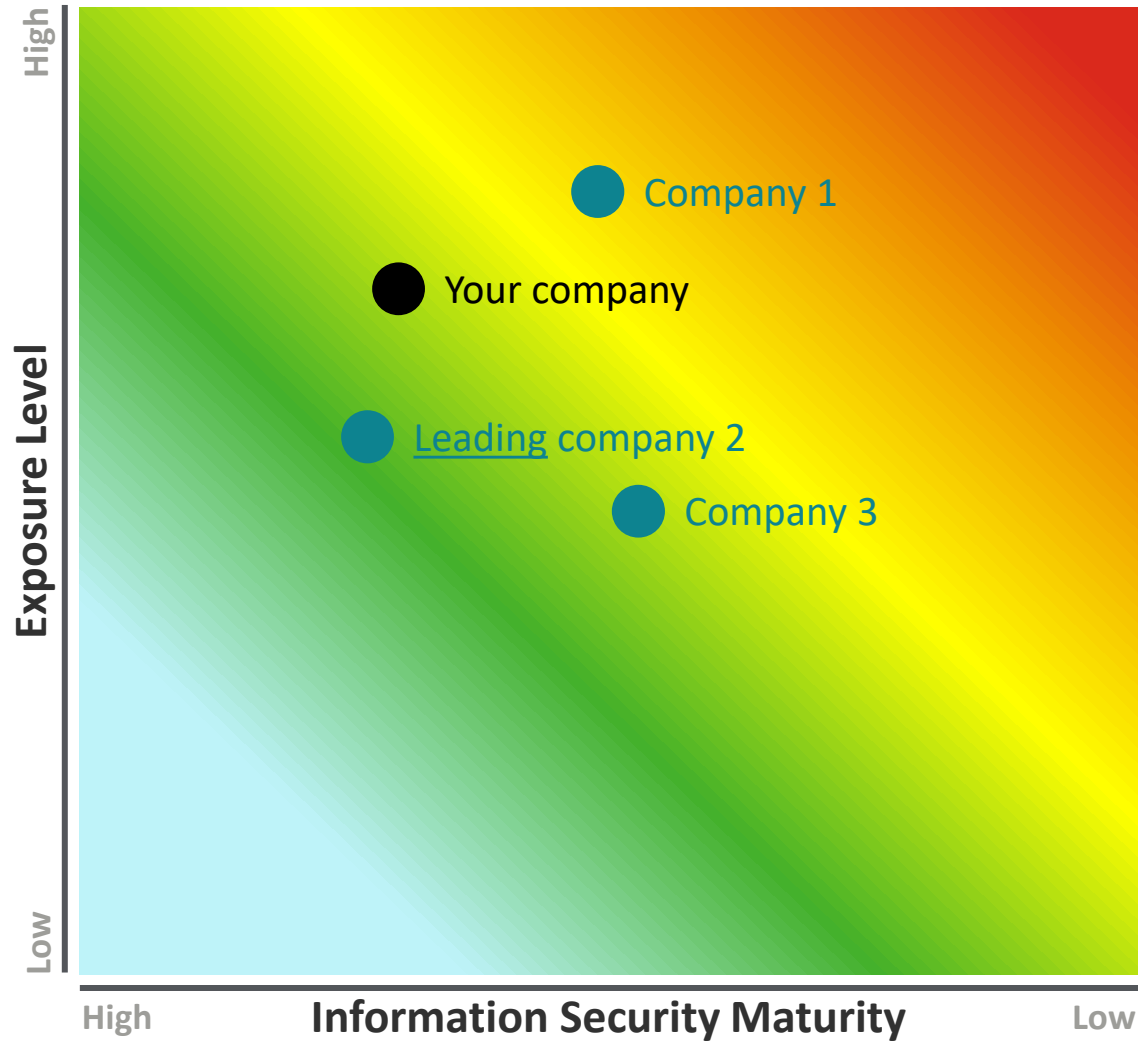
Therefore, the Average Loss provides an indication for the average loss if a loss occurs, in combination with the respective recurrence period.

Example: “If a data breach event occurs, this will be on average every 12 years and will cost an average loss amount of € 17 m.”



# Your Cyber Risk | Your Benchmark

Compare your score with one or multiple peer companies



Looking at similar players in your environment, one player stands out as best, but most are not well positioned in terms of balancing information security against exposure.

Of course, such benchmarking has its limitations. For professional strategic cyber risk management, risk scores are not the best steering mechanism. Therefore, our ciQ approach uses these scores as interim results for the ultimate financial metrics.

### Information

Benchmarking is only possible with companies from which we have sufficient data in order to ensure a valid result. Whether benchmarking is possible at the current time must be evaluated individually for a company/industry.



## Your primary contacts

**Deloitte.**

**Marco Geiger**  
Manager  
Cyber Risk Advisory

Mobile: : +43 664 80 537 3731

mageiger@deloitte.at

**Deloitte Consulting GmbH**

Renngasse 1/Freyung,  
1010 Vienna, Austria  
[www.deloitte.at](http://www.deloitte.at)

**Deloitte.**

**Georg Schwondra**  
Partner  
Cyber Risk Advisory

Mobile: +43 664 80 537 3760

gschwondra@deloitte.at

**Deloitte Consulting GmbH**

Renngasse 1/Freyung,  
1010 Vienna, Austria  
[www.deloitte.at](http://www.deloitte.at)

**Deloitte.**

**Gerald Kattnig**  
Director  
Cyber Risk Advisory

Mobile: +43 664 80 537 3762

gkattnig@deloitte.at

**Deloitte Consulting GmbH**

Renngasse 1/Freyung,  
1010 Vienna, Austria  
[www.deloitte.at](http://www.deloitte.at)